Electronic Warfare
And the Infantryman

CAPTAIN GREGORY O. BODGE

The education of the infantry soldier generally overlooks the field of electronic warfare. Members of the Military Intelligence and Signal branches have become experts in this field, with only a cursory education on its potential and capabilities being passed on to the Infantry.

With the development of faster, smaller, and more powerful microprocessors and components, the basic elements of electronic warfare have become more powerful and more accessible to more people. Even in the consumer electronics industry, items as basic as cellular and wireless telephones have had to become more sophisticated. They have added digital signal processing and spread spectrum transmissions to prevent eavesdropping and jamming. As the speed of computers increases, the length of time needed to detect a soldier on a radio decreases. Every time an infantryman uses something as basic as a radio without taking specific precautions, he must assume that someone knows where he is and on what frequencies he is transmitting. Therefore, it is vital that any member of the infantry who will use a radio, or any other device designed to transmit electromagnetic waves, know the dangers involved and how to reduce them.

Electronic warfare usually covers three broad areas—electronic sensing (ES), direction finding (DF), and jamming or electronic attack (EA).

Electronic sensing is the ability to determine whether an electromagnetic wave is being transmitted. This is the easiest form of electronic warfare to implement, requiring only an antenna and readily available receivers. The design of a direction-finding system enables a receiver to determine the direction and location of a transmitted signal. DF systems are effective against modern military transmitters, difficult and expensive to create, but rudimentary systems can be built with simple meters and directional antennas. This makes DF less of a threat to infantrymen than ES, but in its fundamental state, it is still an option for many potential enemies. Jamming or EA is the means by which an enemy can prevent the reception of a transmitted signal. It can take on many forms, in a variety of costs and sizes, but generally must be large and expensive, to be effective against modern transmitters.

Electronic sensing devices fall into two categories—signal intelligence and communications intercept. Signal intelligence systems can tell the user if someone is broadcasting, the frequency on which he is broadcasting, and the strength of the broadcast signal. Communications intercept systems allow the user to listen to radio communications. Modern spread spectrum systems and encrypted communications are not easily susceptible to communications intercept systems. This does not mean they are not susceptible to signal intelligence systems. Any transmitted signal, regardless of modulation type, frequency, or content, can be detected if not properly transmitted. With today's processing power, even a short-duration encrypted message can give an enemy valuable information, even though he cannot decipher the message.

Building basic direction finding systems at home is a popular hobby with electronics enthusiasts. These systems generally consist of an antenna, designed to receive in one direction, connected to a power meter. Pointing the antenna at a detected signal indicates the direction of the signal by changes in the power level. The power meter will indicate an increase, and the assumption is that the antenna is pointing at the source. The closer the system gets to the source, the more accurate it is. This one dimensional data will give only an azimuth to the target. Coordinating two or more systems to work a specific signal at the same time can give a location. The more systems that are working the signal, the closer the result will be to the actual transmitter location. Several systems receiving one incorrectly operated platoon radio signal will give the enemy a very accurate fix on the platoon's location, and possibly its movement. This can allow the determination of possible objectives, and even targeting.

Electronic attack systems can deny the enemy the ability to use radios effectively. They can be small, low power, battery operated units, or large, high power, multi-frequency systems. They operate on the theory that a high-power transmitter can distort the transmission of a lower power transmitter on the same frequency. These systems usually transmit noise at a high power and at frequencies known to be in use by enemy forces. A major disadvantage of EA systems is that they are also transmitters and are susceptible to direction finding systems.

Soldiers must take specific precautions to defeat EW systems in the field. With a basic understanding of the way various systems work, common sense

can dictate these precautions. A signal cannot be susceptible to listening, jamming, or direction finding without detection. Because of this, the first priority should go to reducing the enemy's detection of the transmitter. Unfortunately, this can also mean making reception more difficult for the intended receiver. One way to overcome this problem is to use the terrain effectively. It is best to place a large terrain feature between the transmitter and the enemy, with no terrain features between the transmitter and the receiver. While this is not always possible, at least a large hill or mountain can be put between the enemy and the transmitter and a small hill between the transmitter and the receiver. Some of the best transmission sites are valleys and draws, which can usually be found in most terrain. If properly positioned, these features will reduce the transmission strength toward the enemy while allowing transmission to the receiver.

When terrain features are not available or not properly oriented, the use of field expedient directional antennas is a good alternative. These use common materials and designs, and formulas for determining antenna lengths can be found in various field manuals. A directional antenna transmits most of the radio's energy in one direction and limits the transmission in other directions. Pointing the antenna toward the intended receiver allows most of the signal strength to go to the receiver. With this system, enemy EW systems will not receive the full signal strength. The most obvious solution to limiting the reception capabilities of the enemy is to reduce the output power of transmitters and reduce transmission time. Most radios used by infantry units have variable power settings. By using the lowest possible setting while still maintaining required communication, it is less likely that the enemy will detect the radio. Unfortunately, this solution requires a change in signal strength while the radio is moving away from the receiver and in varying terrain. The method most easily implemented is reduction of time spent on the radio. If the radio operator limits his transmission time, an EW system has a limited time to collect and analyze data. Operators should spend as little time as possible on the radio and transmit only necessary information. These methods make it difficult for an enemy to receive friendly radio traffic.

While the key to keeping enemy EW systems ineffective is to make signals impossible to detect, this is often difficult to do. The next option, then, is to confuse the enemy systems by making detected signals unusable. Again, terrain can play a key role. Radio waves tend to bounce off hills and buildings, creating a phenomenon known as multipath. Multipath describes the arrival of the same signal at the same point at different times and at different signal strengths. This can cause distortion at the receiver and—because many DF systems use the time the signal arrived to determine direction—difficulty in locating the transmitter. This also means it is more difficult to receive and find the direction of a moving system, particularly one that is moving at constantly changing speeds. Unusable signal information is as good as none at all. And if it can occupy an EW system long enough to keep it from detecting other transmitters, it is better.

Upon the detection of a transmitter, an enemy might decide his best course of action is to jam the transmission frequency. If the radio operator or leaders can guess the jammer's direction, the team should try to put a major terrain feature between themselves and the jamming system. Often the protection the terrain feature can afford will allow clear transmission and reception. The only other option for most units is to change frequencies and take precautions against being detected again. Unfortunately, this often creates confusion throughout the net as operators try to find the new net. Because of these problems and the possibility of disruption, simulated jamming should be incorporated into training whenever possible. If the chain of command is informed of enemy jamming, they can initiate actions to disable the jamming source.

There are times when the mission and the terrain can make it impossible to maintain radio communications without being detected. But even in these instances, it is possible to limit the amount of information that the enemy gathers. Encrypted signals should be used whenever possible to deny the enemy transmitted data. While they will still be able to jam a transmitter or find its direction, they will not know the specifics of the conversation. Retransmission sites will allow operators to transmit at lower power, thus reducing the probability of detection. The high power retransmission site, even if detected by the enemy, will not give him information about specific locations and movements of friendly elements. There are always options to the infantryman for protection from enemy electronic warfare systems.

Some knowledge of electronic warfare systems is vital to mission success. With common sense and precautions, an infantry unit can limit its susceptibility to enemy EW systems, allowing them to complete their missions despite enemy capabilities.

Captain Gregory O. Bodge, when this article was written, was assistant S-3, 54th Troop Command, New Hampshire Army National Guard. He was commissioned from the Massachusetts Military Academy OCS. He gained experience as an electrical engineer supporting Force XXI programs with the 104th Military Intelligence Battalion, 4th Infantry Division. He also served in the 1st Battalion, 104th Infantry, Massachusetts Army National Guard.
